Rules of Use
of the Front Office surface of IMIS 2007-2013

This regulation lays down the requirements of secure application of the IMIS 2007-2013 system (hereinafter referred to as the system). By logging in to the system, the Lead Beneficiary (hereinafter referred to as the User) accepts the following rules.

General rules

– The User is obliged to learn the rules of the proper use of the system and to apply the system according to the User Manual.

– The User is only allowed to complete tasks in line with his/her role within the system.

– The User is obliged to cooperate with the Joint Technical Secretariat in case any examination related to system events becomes necessary.

– The User is responsible for the accuracy of the data entered into the system.

Security rules

– It is prohibited to use any programmes, applications or devices that may affect the operation of the system.

– The User is responsible for the secure use of the system.

– In order to guarantee the safe operation of the system the User is obliged to use a client computer that is sufficiently protected: equipped with central or local firewall, regularly updated antivirus system and well-protected user accounts for the workstation.

– The User is obliged to use a complex password that is kept confidential. The User has to select a password with a length of at least 8 characters, containing lower case letters, capital letters and digits as well. The password shall be changed regularly.

– In case of any activity that endangers the safe operation of the system the access of the affected User will be suspended and IT security examination will be started.

Rules for suspicion of misuse

– In case of unauthorized usage the owner of the user name has to take the responsibility.

– In case of reasonable suspicion of unauthorized usage all the tasks accomplished by the User in the system can be examined during the security examination without preliminary notification.

– In case of a suspicion that the password could be learned by another unauthorized person the User has to change it immediately and he/she has to inform the designated programme manager about this event.

Joint Technical Secretariat, VÁTI Hungarian Nonprofit Limited Liability Company for Regional Development And Town Planning
1016 Budapest, Gellérthegy u. 30-32. Tel: +36 1 224 3272, Fax: +36 1 224 3291, E-mail: jts@huro-cbc.eu
www.hungary-romania-cbc.eu • www.huro-cbc.eu

– If the client computer used for accessing the system is infected by a virus the User is not allowed to log into the system until the infection is eliminated. The Joint Technical Secretariat shall be informed of the virus infection immediately in order to eliminate the virus affection of files uploaded.

– It is prohibited to provide information on any system error or vulnerability to third persons; these issues shall be reporte d immediately to the Joint Technical Secretariat.

Joint Technical Secretariat, VÁTI Hungarian Nonprofit Limited Liability Company for Regional Development And Town Planning
1016 Budapest, Gellérthegy u. 30-32. Tel: +36 1 224 3272, Fax: +36 1 224 3291, E-mail: jts@huro-cbc.eu
www.hungary-romania-cbc.eu • www.huro-cbc.eu